REMARKS

The Office Action dated July 9, 2008, has been received and carefully noted. The above amendments to the claims, and the following remarks, are submitted as a full and complete response thereto.

By this Response, claims 1, 7, 10, 14, and 16-18 have been amended to more particularly point out and distinctly claim the subject matter of the present invention. Claims 9 and 13 have been cancelled without prejudice or disclaimer. Claims 21-26 have been added. No new matter has been added. Support for the above amendments is provided in the Specification at least in paragraphs [0033]-[0037]. Accordingly, claims 1-8, 10-12, and 14-26 are currently pending in the application, of which claims 1, 10, 14, 16, 18, and 21-26 are independent claims.

In view of the above amendments and the following remarks, Applicants respectfully request reconsideration and timely withdrawal of the pending rejections to the claims for the reasons discussed below.

Claim Rejections under 35 U.S.C. §102(e)

The Office Action rejected claims 1-5, 8, 10-16, and 18-20 under 35 U.S.C. §102(e) as allegedly anticipated by Leung, *et al.* (U.S. Patent No. 6,760,444) ("Leung"). The Office alleged that Leung discloses or suggests every feature recited in claims 1-5, 8, 10-16, and 18-20. Applicants respectfully submit that the claims recite subject matter that is neither disclosed nor suggested in Leung.

Claim 1, upon which claims 2-8 depend, recites an apparatus. The apparatus includes an application device, a service device, and a communication network configured to connect the application device to the service device. The apparatus further includes an internet protocol security service unit configured to provide one or more internet protocol security services including at least one of authentication services and encryption services. The internet protocol security service unit is deployed in the service device. The apparatus further includes at least one management client configured to issue security association management requests to create and manage, with a session key management protocol, security associations for use by the provided internet protocol security services. The at least one management client is deployed in the application device. Further, the apparatus includes a management server configured to receive the security association management requests issued from the at least one management client and to respond, in connection with the internet protocol security service unit, to the security association management requests received at the management server. The management server is deployed in the service device.

Claim 10, upon which claims 11-12 depend, recites a method. The method includes providing one or more internet protocol security services including at least one of authentication services and encryption services from an internet protocol security service unit. The internet protocol security service unit is deployed in a service device. The method further includes issuing security association management requests to create and manage, with a session key management protocol, security associations for use by

the provided internet protocol security services, from at least one management client. The at least one management client is deployed in an application device. Further, the method includes receiving in a management server the security association management requests issued from the at least one management client, and responding, in connection with the internet protocol security service unit, to the security association management requests received at the management server. The management server is deployed in the service device. The application device is connected to the service device by a communication network.

Claim 14, upon which claim 15 depends, recites an apparatus. The apparatus includes at least one management client configured to issue security association management requests to create and manage, with a session key management protocol, security associations for use by on or more internet protocol security services including at least one of authentication services and encryption services provided by an internet protocol security service unit external to the apparatus. The apparatus further includes an interface configured to communicate the issued security association management requests to a management server external to the apparatus, The management server is configured to respond to the security association management requests in connection with the internet protocol security service unit.

Claim 16, upon which claim 17 depends, recites an apparatus. The apparatus includes an internet protocol security service unit configured to provide one or more internet protocol security services including at least one of authentication services and

encryption services. The apparatus further includes a management server configured to receive security association management requests issued from at least one management client external to the apparatus and to respond, in connection with the internet protocol security service unit, to the received security association management requests.

Claim 18, upon which claims 19-20 depend, recites a method. The method includes issuing, from at least one management client deployed in an application device, security association management requests to create and manage, with a session key management protocol, security associations for use by one or more internet protocol security services including at least one of authentication services and encryption services provided by an internet protocol security service unit external to the application device. The method further includes communicating at least one of the issued security association management requests to a management server external to the application device. The management server is configured to respond to the security association management requests in connection with the internet protocol security service unit.

As will be discussed below, Leung fails to disclose or suggest each and every element recited in claims 1-5, 8, 10-16, and 18-20, and therefore fails to provide the features discussed above.

Leung is directed to mobile IP authentication. In particular, Leung describes a method and apparatus for authenticating a mobile node. A server is configured t provide a plurality of security associations associated with a plurality of mobile nodes. A packet identifying a mobile node may then be sent to the server from a network device such as a

home agent. A security association for the mobile node identified in the packet may then be sent to the network device to permit authentication of the mobile node. Alternatively, authentication of the mobile node may be performed at the server by applying the security association (Leung, Abstract; col. 4, line 65, to col. 5, line 36).

Applicants respectfully submit that Leung fails to disclose or suggest each and every element recited in claim 1, and similarly recited in claims 10, 14, 16, and 18. In particular, Leung fails to disclose or suggest, at least, "at least one management client configured to issue security association management requests to create and manage, with a session key management protocol, security associations for use by said provided internet protocol security services, said at least one management client deployed in said application device; and a management server configured to receive said security association management requests issued from said at least one management client and to respond, in connection with said internet protocol security service unit, to said security association management requests received at said management server, said management server deployed in said service device," as recited in claim 1, and similarly recited in claims 10, 14, 16, and 18.

The Office Action alleged that Leung discloses the aforementioned claim features, reciting the teachings of Leung at column 2, line 58, to column 3, line 16, and column 7, lines 16-50. However, a review of these passages demonstrates that Leung fails to disclose or suggest each and every element recited in claims 1, 10, 14, 16, and 18.

Rather, Leung, at column 2, line 58, to column 3, line 16, generally discusses RFC 2002. RFC 2002 specifies a packet format for both registration request and registration reply packets that are sent between a mobile node and a home agent. Additionally, these teachings of Leung generally discuss a security-association that defines a key and algorithm to be applied during an authentication process. However, the teachings of Leung fail to disclose or suggest that the home agent *contacts* the server with a request for services, such as creating and managing security associations.

Rather, Leung, at column 2, line 58, to column 3, line 16, specifically discusses the mobile node and the home agent exchanging registration request packets 202 and registration reply packets 204, both of which include Security Parameter Index 212, that is an identifier which specifies a security association, or "row" in a security association table that a receiver should use to interpret a received packet. Hence, Leung teaches indicating a security association that has previously been stored in a security-association table. Therefore, Leung fails to disclose or suggest that the home agent and the mobile node *contact each other* with a request for *creating and managing* security associations.

Similarly, Leung, at column 7, lines 16-50, discusses the home agent obtaining or retrieving the security association from the server in which the security association has been previously stored. Again, Leung fails to disclose or suggest that the home agent and the mobile node *contact each other* with a request for *creating and managing* security associations.

Furthermore, the teachings of Leung, at column 7, lines 16-50, fail to mention that security associations or authentication services are handled by the server's *internet protocol security services*. In fact, Leung fails to disclose or suggest internet protocol security services at all. Rather, Leung clearly describes that "a server handles security associations for a home agent," *i.e.*, Leung indicates that the server acts as a security association repository for the home Agent. Leung further mentions that, in response to receiving a packet identifying the mobile node (e.g., an authorization request packet) from the home agent, the server obtains a security association for the mobile node identified in this packet and sends the security association to the home agent (Leung, col. 7, lines 33-40). The server does not participate in this authentication. Rather, the actual authentication is performed solely by the home agent.

Additionally, Internet protocol security or IPsec is a set of protocols for providing confidentiality services and authentication services to IP traffic. In contrast, the authentication process discussed in Leung relates to a mobile IP protocol, and more particularly to registration of a mobile node with its home agent. One of ordinary skill in the art would understand that the mobile IP protocol discussed in Leung is a completely different technology from IPsec.

Nevertheless, even if the authentication process of the mobile IP protocol discussed in Leung were considered to read upon the authentication processes of IPsec, Leung still fails to disclose or suggest an arrangement, as taught by certain embodiments of the present invention, in which the security association management application is

divided into a management client and a management server (two separate elements), wherein the management server is deployed at a same device with the internet protocol security service unit, and the management client is deployed at another device on its own.

Furthermore, Applicants respectfully submit that it would be improper to conclude that Leung uses a *session* key management protocol from the teachings of Leung that security associations possibly include keys. Since the security association discussed in Leung already defines the key and algorithm to be applied during the authentication process (*e.g.*, Leung; col. 3, lines 6-8), there is no need for a separate key management protocol. Furthermore, even if a key management protocol could be used, Leung fails to provide motivation for it to be a *session* key management protocol.

Accordingly, Leung fails to disclose or suggest, at least, "at least one management client configured to issue security association management requests to create and manage, with a session key management protocol, security associations for use by said provided internet protocol security services, said at least one management client deployed in said application device; and a management server configured to receive said security association management requests issued from said at least one management client and to respond, in connection with said internet protocol security service unit, to said security association management requests received at said management server, said management server deployed in said service device," as recited in claim 1, and similarly recited in claims 10, 14, 16, and 18.

Claims 2-5 and 8 depend from claim 1. Claims 11-12 depend from claim 1. Claim 15 depends from claim 14. Claims 19-20 depend from claim 18. Accordingly, claims 2-5, 11-12, 15, and 19-20 should be allowable for at least their dependency upon an allowable base claim, and for the specific limitations recited therein. Claim 13 was cancelled without prejudice or disclaimer.

Therefore, Applicants respectfully request withdrawal of the rejections of claims 1-5, 8, 10-16, and 18-20 under 35 U.S.C. §103(a) and respectfully submit that claims 1, 10, 14, 16, and 18, and the claims that depend therefrom, are in condition for allowance.

Claim Rejections under 35 U.S.C. §103(a)

The Office Action rejected claims 6-7, 9, and 17 under 35 U.S.C. §103(a) as being allegedly unpatentable over Leung. Applicants respectfully submit that the claims recite subject matter that is neither disclosed nor suggested in Leung.

Leung was discussed above. Applicants respectfully submit that the Office Action failed to establish a *prima facie* case of obviousness to reject claims 6-7, 9, and 17 under 35 U.S.C. §103(a) based on the teachings of Leung.

As previously noted above, Leung fails to disclose or suggest each and every element recited in claim 1 and 16. In particular, Leung fails to disclose or suggest, at least, "at least one management client configured to issue security association management requests to create and manage, with a session key management protocol, security associations for use by said provided internet protocol security services, said at

least one management client deployed in said application device; and a management server configured to receive said security association management requests issued from said at least one management client and to respond, in connection with said internet protocol security service unit, to said security association management requests received at said management server, said management server deployed in said service device," as recited in claim 1, and similarly recited in claim 16.

Claims 6-7 depend from claim 1. Claim 17 depends from claim 16. Accordingly, claims 6-7 and 17 should be allowable for at least their dependency upon an allowable base claim, and for the specific limitations recited therein. Claim 9 was cancelled without prejudice or disclaimer.

Therefore, Applicants respectfully request withdrawal of the rejections of claims 6-7, 9, and 17 under 35 U.S.C. §103(a) and respectfully submit that claims 1 and 16, and the claims that depend therefrom, are in condition for allowance.

CONCLUSION

In conclusion, Applicants respectfully submit that Leung fails to disclose or suggest each and every element recited in claims 1-8, 10-12, and 14-26. The distinctions previously noted are more than sufficient to render the claimed invention unanticipated and non-obvious. It is therefore respectfully requested that all of claims 1-8, 10-12, and 14-26 be allowed, and this present application be passed to issue.

If for any reason the Examiner determines that the application is not now in condition for allowance, it is respectfully requested that the Examiner contact, by telephone, Applicants' undersigned representative at the indicated telephone number to arrange for an interview to expedite the disposition of this application.

In the event this paper is not being timely filed, Applicants respectfully petition for an appropriate extension of time. Any fees for such an extension together with any additional fees may be charged to Counsel's Deposit Account 50-2222.

Respectfully submitted,

Brad Y. Chin
Attorney for Applicants
Registration No. 52,738

Customer No. 32294
SQUIRE, SANDERS & DEMPSEY LLP
14TH Floor
8000 Towers Crescent Drive
Vienna, Virginia 22182-6212
Telephone: 703-720-7800
Fax: 703-720-7802

BYC:dlh

Enclosures: Additional Claim Fee Transmittal
Check No. 019739